

# Data Protection policy

## Policy Statement

Lothian Buses Limited and our subsidiary companies (the Lothian Group) collect and use information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the General Data Protection Regulation (GDPR).

We regard the lawful and correct treatment of personal information as very important to the successful and efficient performance of our functions, and to maintain confidence between those with whom we deal.

To this end, we fully endorse and adhere to the Principles of Data Protection, as set out in GDPR and we have a Data Protection regime in place to oversee the effective and secure processing of personal data.

## Purpose

The purpose of this policy is to ensure that the staff of the Lothian Group are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

Failure to adhere to GDPR is unlawful and could result in legal action being taken against the Lothian Group or its staff or trustees.

## Principles

The General Data Protection Regulation regulates the processing of information relating to living and identifiable individuals (natural persons). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems.

Data users must comply with the data protection principles of good practice which underpin the Regulation. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, the Lothian Group follow the Data Protection Principles outlined in Article 5 of the General Data Protection Regulation, which are summarised below:

Personal data will be processed fairly, lawfully and in a transparent manner in relation to individuals.

Data will only be collected and used for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data will be accurate and, where necessary, kept up to date and every reasonable step will be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes under which it is processed; personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes with safeguards required under GDPR to uphold the rights and freedoms of individuals; and

Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The principles apply to “personal data” which is information held on computer or in manual filing systems from which they are identifiable. Lothian Group employees who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

## **Procedures**

The following procedures have been developed in order to ensure that we meet our responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by us falls into 2 broad categories:

1. Lothian Group’s internal data records;  
Staff

2. Lothian Group’s external data records;  
Customers and suppliers.

Lothian Buses Limited as a body is a Data Controller under the Act, and the Executive Committee is ultimately responsible for the policy’s implementation.

## Internal data records

### **Purposes**

We obtain personal data (names, addresses, phone numbers, email addresses, photographs), and in some cases other documents from staff. This data is stored and processed as per the Employee Privacy Notice.

### **Access**

The contact details of staff will only be made available to other staff.

Contact details of staff will not be passed on to anyone outside the organisation without their explicit consent unless we are legally obliged to do so.

A copy of staff emergency contact details will be kept for Health and Safety purposes to be used in emergency situations e.g. fire/ bomb evacuations. Staff will be supplied with a copy of their personal data held by the organisation if a request is made through our Subject Access Request form on our website or to the Data Protection Officer.

All confidential post must be opened by the addressee only.

### **Accuracy**

We will take reasonable steps to keep personal data up to date and accurate.

Personal data will be stored for up to 6 years after an employee has worked for the organisation after which it will be securely destroyed. The Head of People has responsibility for ensuring the confidential destruction of personnel files.

### **Storage**

Personal data is kept in paper-based systems and on password-protected computer systems.

Every effort is made to ensure that paper-based data are stored in organised and secure filing systems and access limited to relevant personnel.

We operate a clear desk policy at all times.

### **Use of Photographs**

Where practicable, we will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisations website or on internal media outlets.

## External data records

### Purposes

We obtain personal data (such as names, addresses, email addresses, photographs and phone numbers) from customers. This data is obtained, stored and processed solely to assist staff in the efficient running of services. Personal details supplied are only used to send material that is potentially useful after explicit opt in or under legitimate interest.

This information is stored on the organisation's databases and is processed as per our Customer Privacy Notice.

We obtain personal data and information from customers in order to provide services. This data is stored and processed only for the purposes outlined in the agreement and service specification signed by the customer.

### Consent

Personal data is collected over the phone and using other methods such as e-mail or web contact forms. During this initial contact, the data owner is given an explanation of how this information will be used.

Written consent is not requested as it is assumed that the consent has been granted when an individual freely gives their own details.

Personal data will not be passed on to anyone outside the organisation without explicit consent from the data owner unless there is a legal duty of disclosure under other legislation.

### Access

Only the organisation's staff will have access to personal data.

All staff are made aware of the Computer Usage and Information Security Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.

Information supplied is kept in a secure filing, paper and electronic systems and is only accessed by those individuals involved in the delivery of the service.

Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies e.g. the Inland Revenue, or unless there is a legal duty of disclosure under other legislation.

Individuals will be supplied with a copy of any of their personal data held by the organisation if a request is made via our Subject Access Request Form or to the Data Protection Officer.

All confidential post must be opened by the addressee only.

## **Accuracy**

We will take reasonable steps to keep personal data up to date and accurate.

Personal data will be stored for as long as the data owner uses our services and up to 5 years after, as per our Customer Privacy Policy. A copy of our Data Retention Schedule can be requested from our Data Protection Officer at [DPO@lothianbuses.co.uk](mailto:DPO@lothianbuses.co.uk)

Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed according to our Data Retention Schedule.

If a request is received from an organisation/ individual to destroy their records, we will remove/obfuscate/anonomise their details from all databases and ensure that all staff holding paper or electronic details for the organisation securely destroy them. This work will be carried out by the Data Protection Officer.

## **Storage**

Personal data may be kept in paper-based systems and on password-protected computer systems.

Paper-based data are stored in organised and secure filing systems.

We operate a clear desk policy at all times.

## **Use of Photographs**

Where practicable, we will seek consent of members/ individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisation's website or other external media outlets.

## **Responsibilities of staff**

During the course of their duties, staff will be dealing with information such as names/addresses/phone numbers/e-mail addresses/photographs of customers or suppliers. They may be told or overhear sensitive information while working for us. GDPR gives specific guidance on how this information should be dealt with. In short to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

All Staff must abide by this policy.

## Compliance

Compliance with the Regulation is the responsibility of all staff. We will regard any unlawful breach of any provision of GDPR by any staff as a serious matter which may result in disciplinary action. Any employee who breaches this policy statement may be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

## Retention of Data

No documents will be stored for longer than is necessary. For guidelines on retention periods see the Data Retention Schedule.

All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.

### Who to Contact

Any queries with regard to our Data Protection Policy can be directed to our Data Protection Officer at

Data Protection Officer  
Lothian Buses  
55 Annandale Street  
Edinburgh  
EH7 4AZ

Or [DPO@Lothianbuses.co.uk](mailto:DPO@Lothianbuses.co.uk)